CLAIMS

1. An enterprise network architecture, comprising:

a first network system including one or more first network system domains;

a second network system including one or more second network system domains, the second network system being autonomous from the first network system such that the first network system domains are administratively independent from the second network system domains; and

a trust link between a first network system root domain and a second network system root domain, the trust link configured to provide transitive resource access between the one or more first network system domains and the one or more second network system domains.

2. An enterprise network architecture as recited in claim 1, wherein:

the first network system root domain is configured for communication with the one or more first network system domains;

the second network system root domain is configured for communication with the one or more second network system domains; and

the trust link is further configured to provide transitive security associations between the one or more first network system domains and the one or more second network system domains.

3. An enterprise network architecture as recited in claim 1, wherein the transitive resource access includes remote authentication, such that an account managed by the second network system can initiate a request for authentication via a first network system domain.

4. An enterprise network architecture as recited in claim 1, wherein the transitive resource access includes remote authentication to access a resource managed in the second network system, such that an account managed by the second network system can initiate a request for authentication to access the resource via a first network system domain.

5. An enterprise network architecture as recited in claim 1, wherein:

a first network system domain includes a first domain controller;

a second network system domain includes a second domain controller; and

an account managed by the second domain controller can initiate a request for remote network authentication via the first domain controller.

6. An enterprise network architecture as recited in claim 1, wherein:

a first network system domain includes a first domain controller;

a second network system domain includes a second domain controller; and

an account managed by the second domain controller can initiate a request for authentication to access a resource managed in the second network system, the request for authentication communicated from the first domain controller to the second network system via the trust link.

7. An enterprise network architecture as recited in claim 1, wherein:

the first network system root domain is configured for communication with the one or more first network system domains, an individual first network system domain including a first domain controller;

the second network system root domain is configured for communication with the second network system domains, an individual second network system domain including a second domain controller; and

an account managed by the second domain controller can initiate a request for authentication to access a resource managed by the second domain controller, the request for authentication communicated from the first domain controller to the second domain controller via the first network system root domain, the trust link, and the second network system root domain.

8. An enterprise network architecture as recited in claim 1, wherein the trust link is a one-way trust link initiated by an administrator of the first network system, and wherein an account in the second network system can access resources in the first network system.

9. An enterprise network architecture as recited in claim 1, wherein the trust link is a one-way trust link initiated by an administrator of the first network system, the one-way trust link configured to provide transitive resource access from the second network system domains to the first network system domains.

10. An enterprise network architecture as recited in claim 1, wherein the trust link is a two-way trust link initiated by a first network system administrator and by a second network system administrator, and wherein the transitive resource access is automatically configured when the trust link is established.

11. An enterprise network architecture as recited in claim 1, wherein the first network system is configured to determine from the trust link where to communicate a request for a resource, the request received from an account managed in the first network system and the resource maintained by the second network system.

12. An enterprise network architecture as recited in claim 1, wherein the second network system is configured to determine from the trust link where to communicate an authentication request resulting from access to a resource, the request received for an account managed in the first network system and the resource maintained by the second network system, and wherein the second network system is configured to authorize the request for the resource.

13. An enterprise network architecture as recited in claim 1, wherein the first network system is configured to receive a request to logon to the second network system and determine from the trust link where to communicate the request, and wherein the second network system is configured to authenticate the request.

14. An enterprise network architecture as recited in claim 1, wherein the trust link is a data structure configured to maintain namespaces corresponding to trusted network system domain components.

15. An enterprise network architecture as recited in claim 1, wherein the trust link includes a first network system data structure and a second network system data structure, the first network system data structure configured to maintain trusted namespaces corresponding to the second network system, and the second network system data structure configured to maintain trusted namespaces corresponding to the first network system.

16. An enterprise network architecture as recited in claim 1, wherein the trust link is a data structure configured to maintain namespaces corresponding to the second network system, and wherein the first network system is configured to maintain the data structure and automatically designate which of the namespaces are trusted by the first network system.

17. An enterprise network architecture as recited in claim 1, wherein the trust link is a data structure maintained by the first network system, the data structure configured to maintain namespaces corresponding to trusted second network system domain components, and the trusted second network system domain components being designated as trusted by a first network system administrator.

18. An enterprise network architecture as recited in claim 1, wherein the trust link is a data structure maintained by the first network system, the data structure configured to maintain trusted namespaces corresponding to the second network system, and wherein the first network system is configured to receive a request to logon to the second network system and determine from the trusted namespaces where to communicate the request.

19. An enterprise network architecture as recited in claim 1, wherein:

the trust link is a data structure maintained by the first network system, the data structure configured to maintain trusted namespaces corresponding to the second network system; and

the second network system is configured to determine from the trusted namespaces where to communicate an authentication request resulting from access to a resource, the request received for an account managed in the first network system and the resource maintained by the second network system.

20. An enterprise network architecture as recited in claim 1, wherein:

the trust link is a data structure maintained by the first network system, the data structure configured to maintain trusted namespaces corresponding to the second network system;

the second network system is configured to determine from the trusted namespaces where to communicate an authentication request resulting from access to a resource, the request received for an account managed in the first network system and the resource maintained by the second network system; and

the second network system is configured to authorize the request for the resource.

21. An enterprise network architecture as recited in claim 1, wherein the first network system is configured to:

receive an account request to logon to the second network system;

determine from the trust link where to communicate the account request; and

provide a security identifier to the second network system, the security identifier corresponding to the account.

22. An enterprise network architecture as recited in claim 1, wherein:

the first network system is configured to determine from the trust link where to communicate a service account request to access a resource maintained by the second network system;

the first network system is further configured to provide a security identifier to the second network system, the security identifier corresponding to a user account maintained by the first network system; and

the second network system is configured to determine from the trust link whether to trust the security identifier to authorize the service account request.

23. An enterprise network architecture as recited in claim 1, wherein the trust link is a data structure maintained by the first network system, the data structure configured to maintain trusted namespaces corresponding to the second network system, and wherein the first network system is configured to:

determine from the trusted namespaces where to communicate a logon request received from an account managed in the second network system; and

provide a security identifier to the second network system, the security identifier corresponding to the account.

24. An enterprise network architecture as recited in claim 1, wherein the trust link is a data structure maintained by the first network system, the data structure configured to maintain trusted namespaces corresponding to the second network system, and wherein:

the first network system is configured to determine from the trusted namespaces where to communicate a service account request to access a resource maintained by the second network system;

the first network system is further configured to provide a security identifier to the second network system, the security identifier corresponding to a user account maintained by the first network system; and

the second network system is configured to determine from the trusted namespaces whether to trust the security identifier to authorize the service account request.

25. A data structure, comprising:

one or more namespace records configured to define a trust link between a network system and an autonomous trusted network system, an individual namespace record including:

a namespace field to maintain a namespace corresponding to the trusted network system;

a namespace data field to maintain a value that identifies the namespace; and

a flag field to maintain an indicator that identifies whether the namespace is trusted.

26. A data structure as recited in claim 25, wherein the individual namespace record further includes a time stamp field to maintain a value that identifies when the individual namespace record is created.

27. A data structure as recited in claim 25, wherein the individual namespace record further includes a pointer field to maintain a reference to the trusted network system.

28. A data structure as recited in claim 25, wherein the namespace field maintains a top level hierarchical namespace managed by the trusted network system.

29. A data structure as recited in claim 25, wherein the namespace field maintains a domain identifier namespace corresponding to a domain in the trusted network system.

30. A data structure as recited in claim 25, wherein the namespace field maintains a domain identifier namespace corresponding to a domain in the trusted network system, and wherein the associated namespace data field maintains values including a domain name service name, a netbios name, and a domain security identifier.

31. A data structure as recited in claim 25, wherein the namespace field maintains an excluded namespace that identifies a domain subtree excluded from a top level hierarchical namespace maintained in a second namespace record.

32. A network system domain, comprising:

a root domain controller communicatively linked with one or more network system domains in a first network system; and

a trusted domain component configured to define a trust link between the root domain controller and a second network system root domain controller, the second network system root domain controller communicatively linked with one or more second network system domains that are administratively independent from the first network system domains, and the trust link being configured to provide transitive resource access between the first network system domains and the second network system domains.

33. A network system domain as recited in claim 32, wherein the root domain controller is configured to create the trusted domain component when the trust link is initiated.

34. A network system domain as recited in claim 32, wherein the root domain controller is configured to establish the transitive resource access between the first network system domains and the second network system domains when the trust link is initiated.

35. A network system domain as recited in claim 32, wherein the trusted domain component defines a one-way trust link from the root domain controller to the second network system root domain controller.

36. A network system domain as recited in claim 32, wherein the trusted domain component is further configured to provide remote network authentication, such that an account managed by a second network system domain can initiate a request for authentication via a network system domain in the first network system.

37. A network system domain as recited in claim 32, wherein the trusted domain component is further configured to provide remote authentication to access a resource managed by a second network system domain, such that an account managed by a first network system domain can initiate a request to access the resource via the network system domain , the request communicated from the root domain controller to the second network system root domain controller via the trust link.

38. A network system domain as recited in claim 32, wherein the root domain controller is configured to determine from the trusted domain component where to communicate a request for authentication received from an account managed by a second network system domain.

39. A network system domain as recited in claim 32, wherein the trusted domain component is configured to indicate where to communicate a request for authentication received from an account managed by a second network system domain.

40. A network system domain as recited in claim 32, wherein the root domain controller is configured to determine from the trusted domain component where to communicate a request for a resource, the request received from an account managed by a second network system domain and the resource maintained by the second network system domain.

41. A network system domain as recited in claim 32, wherein the root domain controller is configured to receive a request to logon to a second network system domain, and determine from the trusted domain component to communicate the request to the second network system root domain controller via the trust link.

42. A network system domain as recited in claim 32, wherein the trusted domain component is a data structure configured to maintain trusted namespaces corresponding to the second network system.

43. A network system domain as recited in claim 32, wherein the trusted domain component is a data structure configured to maintain namespaces corresponding to trusted second network system domain components.

44. A network system domain as recited in claim 32, wherein the trusted domain component is a data structure configured to maintain namespaces corresponding to the second network system, and wherein the root domain controller is configured to maintain the data structure and automatically designate which of the namespaces are trusted by the first network system.

45. A network system domain as recited in claim 32, wherein the trusted domain component is a data structure maintained by the root domain controller, the data structure configured to maintain namespaces corresponding to the second network system, and the namespaces being designated as trusted by a network system administrator.

46. A network system domain as recited in claim 32, wherein the trusted domain component is a data structure maintained by the root domain controller, the data structure configured to maintain trusted namespaces corresponding to the one or more second network system domains, and wherein the root domain controller is configured to receive a request to logon to the second network system and determine from the trusted namespaces where to communicate the request.

47. A network system domain as recited in claim 32, wherein the trusted domain component is a data structure configured to maintain trusted namespaces corresponding to the second network system, and wherein the root domain controller is configured to determine from the trusted namespaces where to communicate a request for a resource, the request received from an account managed by the root domain controller and the resource maintained by a second network system domain.

48. A network system domain as recited in claim 32, wherein:

the trusted domain component is a data structure configured to maintain trusted namespaces corresponding to the second network system;

the root domain controller is configured to determine from the trusted namespaces where to communicate a request for a resource, the request received from an account managed by the root domain controller and the resource maintained by a second network system domain; and

the second network system is configured to authorize the request for the resource.

49. A network system domain as recited in claim 32, wherein the root domain controller is configured to:

receive an account request to logon to a second network system domain;

determine from the trusted domain component where to communicate the account request; and

provide a security identifier to the second network system domain controller, the security identifier corresponding to the account.

50. A network system domain as recited in claim 32, wherein the trusted domain component is a data structure maintained by the domain controller, the data structure including trusted namespaces corresponding to the second network system, and wherein the root domain controller is configured to:

determine from the trusted namespaces where to communicate a logon request received from an account managed by a second network system; and

provide a security identifier to the second network system domain controller, the security identifier corresponding to the account.

51. A first network system domain controller performing a method comprising:

establishing a trust link with a second network system domain controller to provide transitive resource access between domains in a first network system and domains in a separate, autonomous second network system;

receiving an authentication request from an account managed by a domain in the second network system; and

determining to authenticate the request via the trust link.

52. A method as recited in claim 51, wherein establishing the trust link comprises:

receiving network system identifiers corresponding to the second network system;

creating a data structure to maintain the network system identifiers; and

designating which of the network system identifiers to trust.

53. A method as recited in claim 51, wherein establishing the trust link comprises:

receiving namespaces corresponding to the second network system;

creating a data structure to maintain the namespaces; and

designating which of the namespaces to trust.

54. A method as recited in claim 51, wherein establishing the trust link comprises:

receiving network system identifiers corresponding to the second network system;

creating a data structure to maintain the network system identifiers;

determining whether to trust an individual network system identifier; and

designating in the data structure whether to trust the individual network system identifier.

55. A method as recited in claim 51, wherein establishing the trust link comprises:

receiving namespaces corresponding to the second network system;

creating a data structure to maintain the namespaces;

determining whether to trust an individual namespace; and

designating in the data structure whether to trust the individual namespace.

56. A method as recited in claim 51, wherein establishing the trust link comprises:

receiving network system identifiers corresponding to the second network system;

comparing a received network system identifier with existing network system identifiers to determine whether to accept the received network system identifier; and

creating a data structure to maintain accepted network system identifiers.

57. A method as recited in claim 51, wherein establishing the trust link comprises:

receiving namespaces corresponding to the second network system;

comparing a received namespace with existing namespaces to determine whether to accept the received namespace; and

creating a data structure to maintain accepted namespaces.

58. A method as recited in claim 51, wherein establishing the trust link comprises receiving network system identifiers corresponding to the second network system and designating which of the network system identifiers to trust, and wherein determining comprises comparing a component of the request with the network system identifiers to determine that the account is managed in the second network system.

59. A method as recited in claim 51, further comprising providing a security identifier corresponding to the account to the first network system domain controller, the first network system domain controller comparing the security identifier with stored network system identifiers to determine whether the security identifier is valid.

60. A first network system domain controller performing a method comprising:

establishing a trust link with a second network system domain controller to provide transitive resource access between domains in a first network system and domains in a separate, autonomous second network system;

receiving a resource request from an account managed by the first network system domain controller;

determining to communicate the resource request to the second network system; and

communicating the resource request to the second network system domain controller via the trust link.

61. A method as recited in claim 60, wherein establishing the trust link comprises:

receiving network system identifiers corresponding to the second network system;

creating a data structure to maintain the network system identifiers; and

designating which of the network system identifiers to trust.

62. A method as recited in claim 60, wherein establishing the trust link comprises:

receiving namespaces corresponding to the second network system;

creating a data structure to maintain the namespaces; and

designating which of the namespaces to trust.

63. A method as recited in claim 60, wherein establishing the trust link comprises receiving network system identifiers corresponding to the second network system and designating which of the network system identifiers to trust, and wherein determining comprises comparing a component of the request with the network system identifiers to determine that the resource is managed in the second network system.

64. A method as recited in claim 60, further comprising providing a security identifier corresponding to the account to the first network system domain controller, the first network system domain controller comparing the security identifier with stored network system identifiers to determine whether the security identifier is valid.

65. One or more computer-readable media comprising computer-executable instructions that, when executed, direct a first network system domain controller to perform a method comprising:

establishing a trust link with a second network system domain controller to provide transitive resource access between domains in a first network system and domains in a separate, autonomous second network system;

receiving a resource request from an account managed by a domain controller in the second network system;

determining to communicate the resource request to the second network system; and

communicating the resource request to the second network system domain controller via the trust link.

66. One or more computer-readable media as recited in claim 65, wherein establishing the trust link comprises:

receiving network system identifiers corresponding to the second network system;

creating a data structure to maintain the network system identifiers; and

designating which of the network system identifiers to trust.

67. One or more computer-readable media comprising computer-executable instructions that, when executed, direct a domain controller in a first network system to perform a method comprising:

requesting network system identifiers corresponding to a second network system to create a trust link between the first network system and the second network system, the second network system being autonomous from the first network system;

determining whether to accept the network system identifiers;

designating accepted network system identifiers as trusted with trust indicators; and

creating a data structure to maintain the accepted network system identifiers and corresponding trust indicators.

68. One or more computer-readable media as recited in claim 67, wherein determining comprises comparing an individual network system identifier with existing network system identifiers and rejecting the individual network system identifier if it is a duplicate of an existing network system identifier.

69. One or more computer-readable media as recited in claim 67, the method further comprising:

receiving an authentication request to logon to a domain in the second network system;

comparing a component of the authentication request with the network system identifiers; and

communicating the authentication request to the second network system if the component corresponds to a trusted network system identifier.

70. A domain controller in a first network system performing a method, comprising:

receiving a security identifier from a domain controller in a second network system via a trust link, the security identifier corresponding to an account managed by the second network system;

determining whether the security identifier is valid; and

trusting the account corresponding to the security identifier if the security identifier is determined to be valid.

71. A method as recited in claim 70, wherein determining comprises comparing the security identifier with network system identifiers and determining that the security identifier is valid if it matches a component of a network system identifier.

72. A method as recited in claim 70, wherein determining comprises comparing the security identifier with stored network system identifiers and determining that the security identifier is valid if it matches a component of a network system identifier, the network system identifiers received from the second network system and designated as being trusted when the trust link is initiated.

73. A method as recited in claim 70, wherein the security identifier corresponds to a security principal managed by the domain controller in the second network system.

74. One or more computer-readable media comprising computer-executable instructions that, when executed, direct a computing system to perform the method of claim 70.